MCOTEA Strategy for OT&E of Interoperability, E3/SM, Security and Information Assurance

Prepared for: AAAV Team

Prepared by: Mr. Peter H. Christensen

Assistant Scientific Advisor

Marine Corps Operational Test and Evaluation Activity

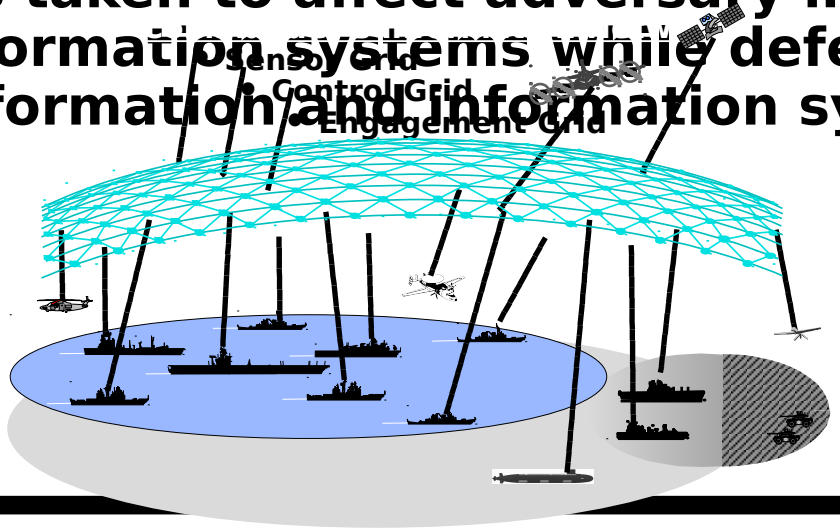
Thursday, May 09, 2002

Summary Slide

- Background: DOD Joint Vision and Information Assurance
- Leveraging The Acquisition Process
- Key Policies
- DOD CIO Policy
- IA OT Policy
- Security
- Joint Interoperability
- Electromagnetic Environmental Effects and Spectrum Management (E3/SM)
- Roles and Responsibilities
- Conclusions

Background: Joint Vision 2010

- **DOD Joint Vision: Focus is Network Centric Warfare (NCW)**
  - **NCW relies on distributed platforms and sensors to detect, locate, target and eliminate enemy with precision munitions**
- **NCW is dependent upon effective Information Operations**
  - **Actions taken to affect adversary information and information systems while defending ones own information and information systems**

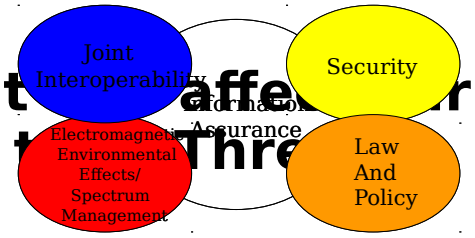


The Emerging Challenge: Information Assurance

- **Information Assurance (IA):**
  - **A subset of Information Operations (IO)**
  - **Protects and defends information and information systems (IS) by ensuring their *availability, integrity, confidentiality, authentication, non-repudiation***
  - **Includes providing for the restoration of IS by incorporating *protection, detection and reaction capabilities***
- **Without effective Information Assurance:**
  - **Simply disrupting the network isolates sensors from weapon systems and impairs your fighting ability!**
  - **Infiltrating the network could allow the enemy to exploit your sensors and understand your force disposition**

IA Interdependencies

- **IA is directly related to other system characteristics**
  - **Service and Joint Interoperability requirements establish the *context within which we execute IO* and evaluate IA Posture**
  - **Electromagnetic Environmental Effects (E3) impact the *availability and integrity* of IO**
  - **RF spectrum may be required to effect IO and must be reserved, *available* and managed**
  - **System Security affects *availability, integrity, confidentiality, authentication, non-repudiation of IO***
- **All of the above are interdependent affe[illegible] ability to detect, protect and react t[illegible] Thre[illegible]**



Leveraging The Acquisition Process and Products

- **DRPM AAAV is responsible for developing the AAAV material solution**
  - **DRPM confirms AAAV requirements are satisfied through the Acquisition Process and during Developmental Test (DT)**
- **MCOTEA is responsible for confirming that the AAAV is operationally effective (OE) and suitable (OS)**
  - **MCOTEA conducts Operational Testing (OT) as required**
- **AAAV testing requirements are allocated to DT and OT as part of the testing process**
  - **When properly coordinated, MCOTEA can leverage products that are generated by DRPM AAAV as part of the acquisition process and DT**
  - **Leveraging the acquisition process to support testing minimizes cost and contributes to timely fielding of a secure, interoperable AAAV**

Leveraging the Acquisition Process and Products for IA

- MCOTEA has identified 25 different instructions that address Security, Interoperability, E3/SM and IA
- MCO 3093.1C; Intraoperability/Interoperability of Marine Corps Tactical C4I Systems
- SECNAVINST 5239.3; DON INFOSEC Program
- Other key documents:
  - DOD CIO GIG IA Policy Memo. No. 6-8510 (16 June 2000)
    - DOD 8500 IA Directive in final draft
  - DOT&E Policy for OT&E of IA (17 Nov 1999)
  - DOD 8510.1 DITSCAP Application Manual (31 July 2000)
  - CJCSI 6212.01B Interoperability and Supportability of NNSS and IT Systems (08 May 2000)
  - DOT&E Assessment Guide for E3/SM Operational Testing (13 June 2001)
- Challenge : Incorporate 25 Inst. into cohesive test strategy!

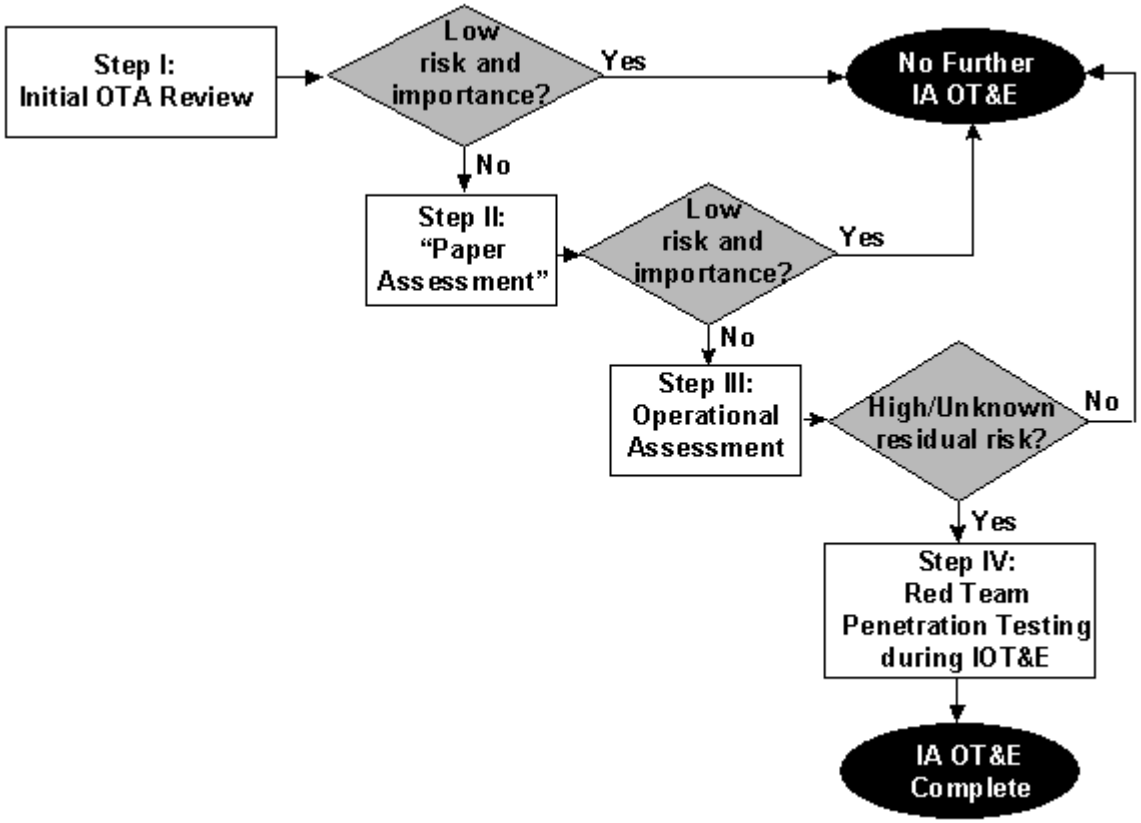
DOD IA Policy and Impact

- DOD IA Policy helps MCSC and MCOTEA to develop a frame of reference for dealing with a specific systems
- Current Policy includes
  - DOD CIO GIG IA Policy 16 June 2000 Memo. No. 6-8510.
    - Implements Clinger-Cohen Act within DOD
  - DoDD 5200.28 – “Security Requirements for AISs”
  - DoD 5200.28-M – “ADP Security Manual”
- DOD CIO Policy establishes Information System Mission Categories, Level of Concern and Level of Robustness!
  - AAAV is clearly Mission Critical!
- DoDD 8500.aa will supercede above policies
  - Establishes “Mission Categories”
    - AAAV would be classified as Category I or II

DOT&E IA OT Policy

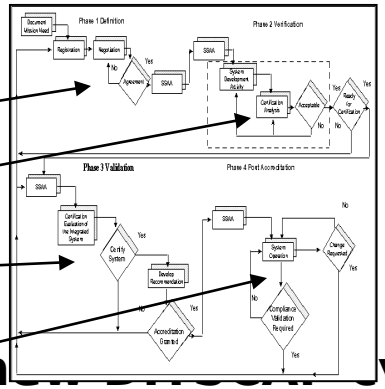
- Policy for Operational Test and Evaluation of Information Assurance (17 Nov 1999)
  - Provides Background, Applicability and Scope, Definitions and Implementation
    - Since been transitioned to DOD 5000.2R
- Applicability : ACAT 1 Programs and programs with DOT&E oversight that have yet to reach MS “C”
  - ***MCOTEA is leveraging this policy to help structure our IA OT strategy***
- Policy describes four implementation steps
  - Step I: Requirements, Threat and Test Documentation Review
  - Step II: Test Strategy Development
  - Step III: Review IA DT&E and Computer Security Certification Results Prior to Entry into OT&E
  - Step IV: Evaluation of IA Vulnerabilities during IOT&E

DOT&E IA OT Four Step Process

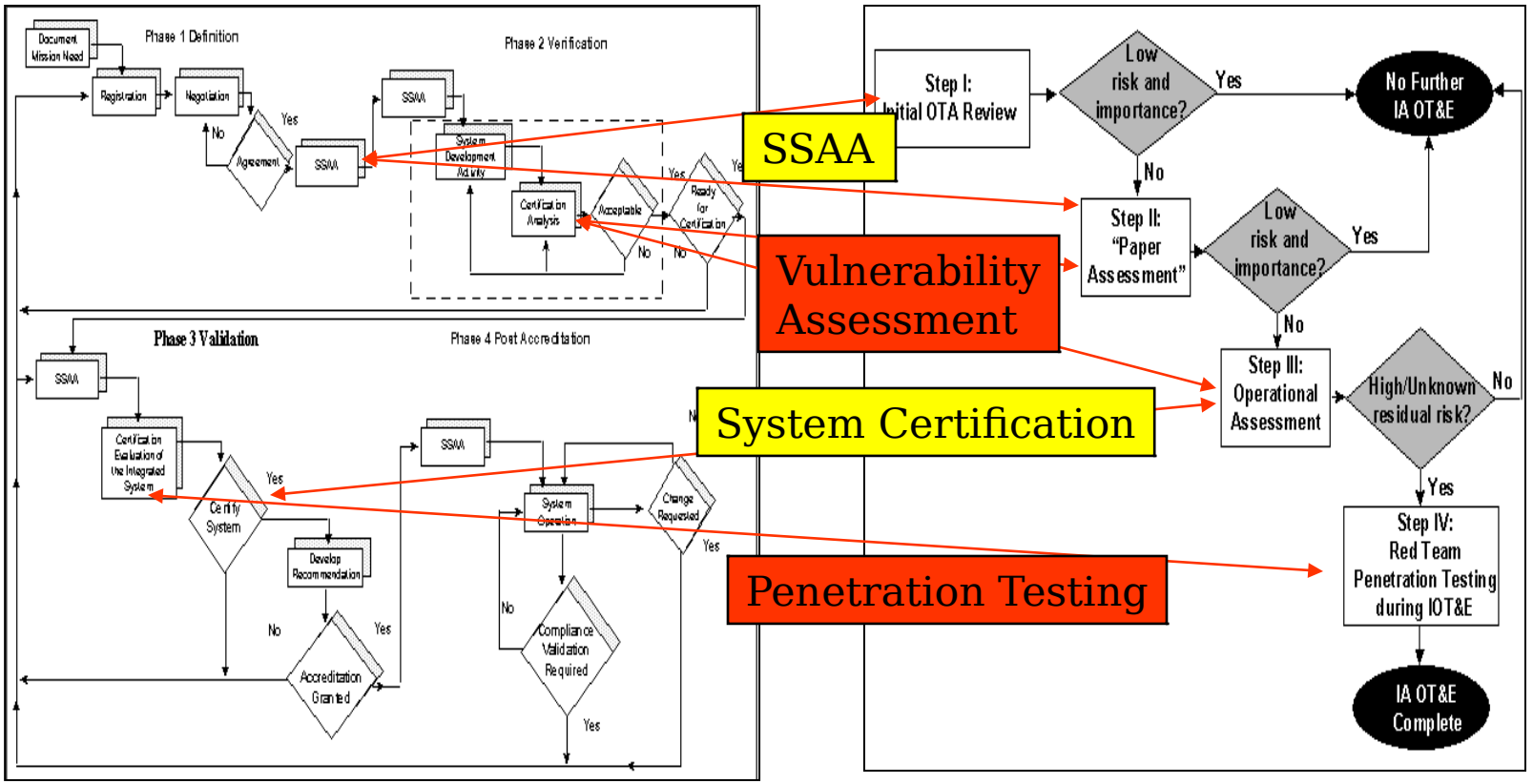


Security

- DoD Information Technology Security Certification and Accreditation Process (DITSCAP) DoD 8510.1
  - All IS, to include stand-alone personal computers, connected systems, and networks, must be accredited
  - The standard DoD Approach for identifying information security requirements, providing security solutions, and managing information technology system security
- USMC Project Officer's Certification and Accreditation Handbook (Sep 2000)
- Four Phase Process
  - Phase 1: Definition
  - Phase 2: Verification
  - Phase 3: Validation
  - Phase 4: Post Accreditation
- Changes to the baseline drive a new DITSCAP cycle



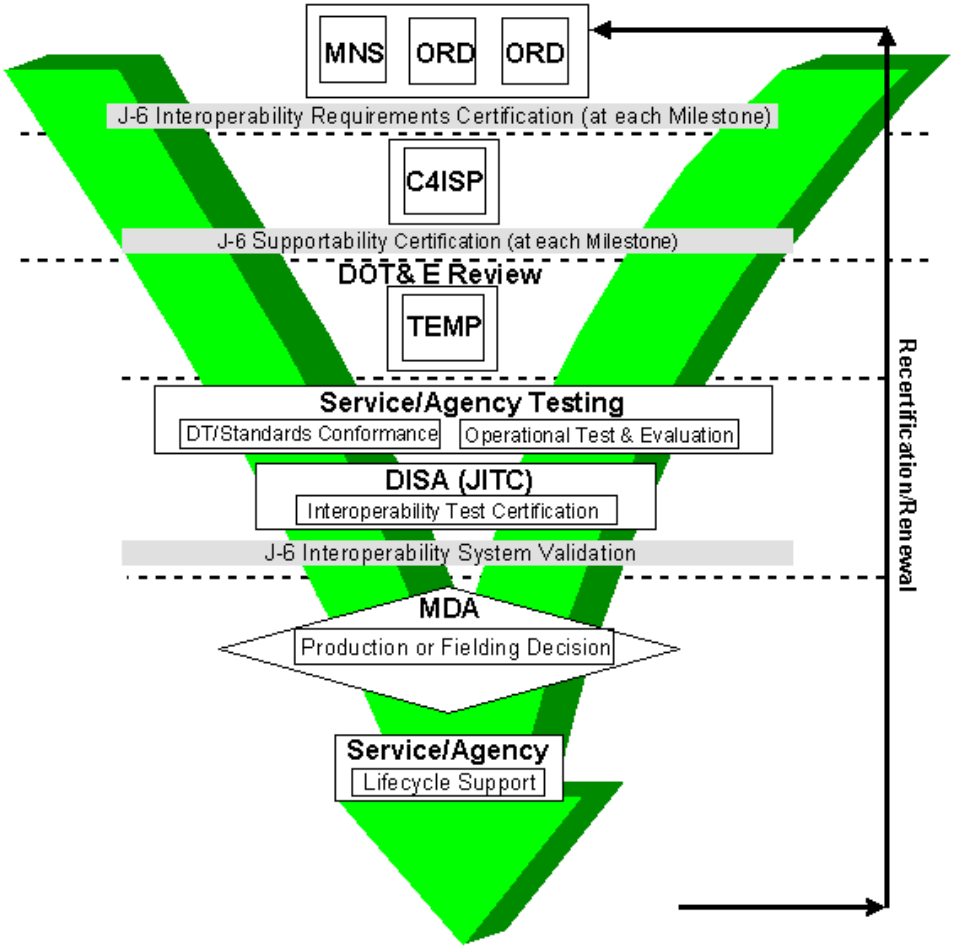
Leveraging DITSCAP for IA



Joint Interoperability

- CJCSI 6212.01B Interoperability and Supportability of National Security Systems and Information Technology Systems (08 May 2000)
  - Establishes policies and procedures for J-6
    - Interoperability requirements certification of MNS, CRD and ORDs
    - Supportability certification of C4ISPs
    - Interoperability system validation
  - Details a methodology to develop interoperability KPPs derived from a set of top-level IERs based on the format and content of the C4ISR integrated architecture products
- JTA Compliance and E3/SM are evaluated as part of this process

Joint Interoperability Certification and Validation Process



Identifies key systems which must exchange information in an operational context!
Evaluates Clinger Cohen, E3, SM, JTA and IA Policy Compliance
Supports TEMP and Test Concept Development.

Joint Interoperability Certification satisfies a Key Performance Parameter!

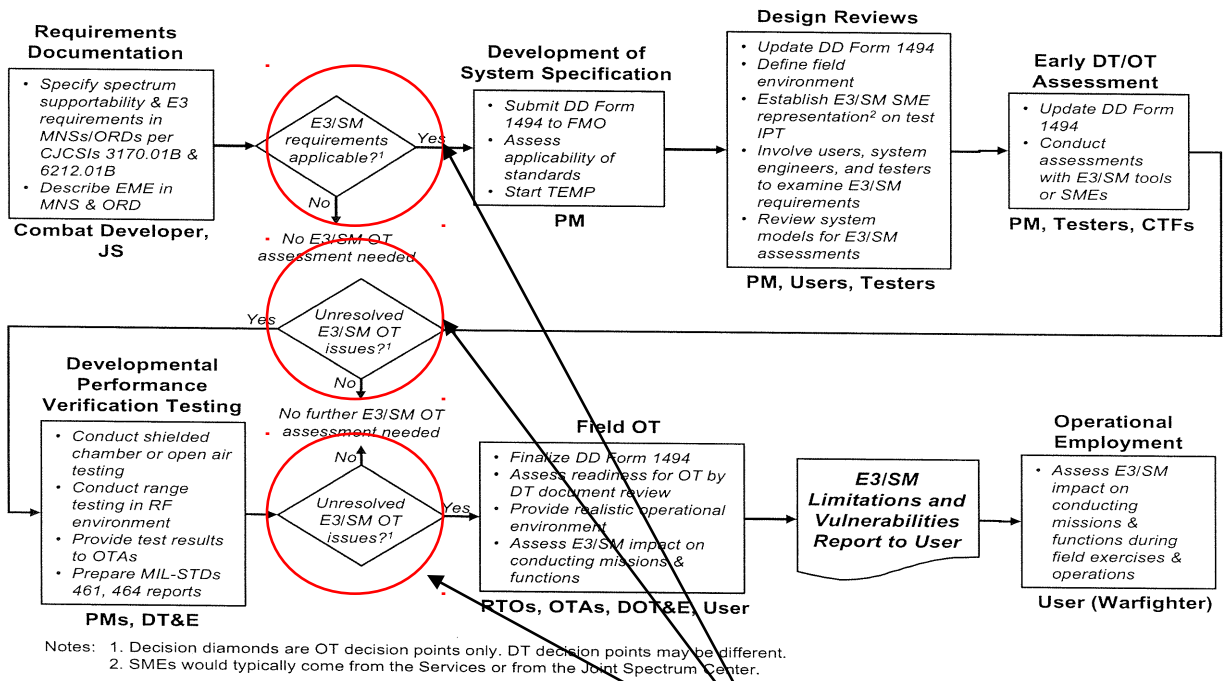
Changes after fielding may drive multiple iterations of Joint Interoperability Certification that may include Security and IA Testing!

Note: Figure from CJCSI 6212.01B

Electromagnetic Environmental Effects and Spectrum Management (E3/SM)

- **E3: The impact of the electromagnetic environment upon the operational capability of military forces, equipment, systems and platforms.**
- **SM: Planning, coordinating and managing the use of the electromagnetic spectrum through operational, engineering and administrative procedures, with the objective of enabling electronic systems to perform their functions in the intended environment without causing or suffering unacceptable interference**
- **DOT&E has developed and Assessment Guide for E3/SM Operational Testing: 13 June 2001**
  - **– Cooperative effort between OSD and Services**
    - **Supports Joint Staff Interoperability Initiatives and references CJCSI 3170.01B and 6212.01B**
  - **– Standardizes the process and provides a checklist!**

DOT&E E3/SM OT Process



From DOT&E E3 and SM Assessment Guide for Operational Testing dated 13 June 01

AAAV Roles and Responsibilities

- **DRPM AAAV will manage the DITSCAP Process, Joint Interoperability, and E3/SM testing**
  - **MCOTEA will use this information to resolve testing issues and reduce the scope of dedicated OT Events**
- **DRPM AAAV will initiate:**
  - **DITSCAP Process**
  - **Joint Interoperability Testing and Certification**
  - **E3 Testing**
  - **SM Testing**

MCOTEA Roles and Responsibilities

- When MCOTEA is the Lead Test Agency
  - MCOTEA will leverage development activities including:
    - DITSCAP Process
    - Joint Interoperability
    - E3/SM Testing
  - MCOTEA will conduct IA OT as appropriate
- When MCOTEA is not the Lead Test Agency
  - MCOTEA will coordinate with the USMC Developing Agency (DA) to resolve Security, Interoperability, E3/SM, and IA Issues during development
    - USMC DA will coordinate with the Lead DA
  - MCOTEA will coordinate with the MTT Lead OTA to leverage development activities and to conduct IA OT

Conclusions

- The strategy discussed here is being formalized between MARCORSYSCOM and MCOTEA via MOU
- IA helps ensure that the AAAV can fight in all environments!
  - Directly supports Joint Interoperability initiatives!
- Several AAAV Developmental MCSC activities are leveraged to quantify IA Posture
  - AAAV DT at the MCTSSA Systems Integration Environment will be exploited to specifically support IA and Joint Interoperability Testing
    - VV&A of SIE as implemented to support AAV is planned
- Questions?

Backups

DOD CIO Policy

- DOD CIO GIG Policy 16 June 2000 Memo. No. 6-8510.
  - Implements Clinger-Cohen Act within DOD
  - Provides direction and assigns responsibilities for secure, interoperable information capabilities
- GIG Definition: “a globally interconnected, end to end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers and support personnel.”
- Applicable to all information technologies used to process, store, display or transmit DOD information, regardless of classification or sensitivity